

EC

page 1

RICHARD V. NAGEL
CLERK OF COURT

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

2021 SEP -2 PM 12:17

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*
Digital devices that were obtained from James SABOLICK,
300 Coon Run Road, Lower Salem, OH, or
7415 Germantown, Lower Salem, OH, which and are
currently being held at 309 4th Street in Marietta, OH

Case No.

2:21-mj-580

U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
EAST. DIV. COLUMBUS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment A, Incorporated herein by reference

located in the Southern District of Ohio, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
 contraband, fruits of crime, or other items illegally possessed;
 property designed for use, intended for use, or used in committing a crime;
 a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section 18 U.S.C. §§ 2251, 2252, and 2252A *Offense Description* Production, Distribution, Receipt, and/or Possession of visual depictions of a minor engaged in sexually explicit conduct and/or child pornography.

18 U.S.C. §§ 2423 Transportation of a Minor Individual for Illicit Sexual Conduct
The application is based on these facts:

See attached affidavit incorporated herein by reference

- Continued on the attached sheet.
 Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Kyle Galbreath, HS1

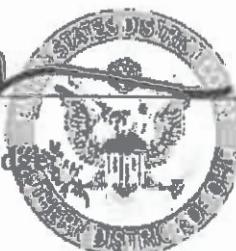
Printed name and title

Sworn to before me and signed in my presence.

Date: September 2, 2021

City and state: Columbus, Ohio

Kimberly A. Johnson
United States Magistrate Judge



UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO,
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF:) Case No:
Digital devices as listed in Attachment A that were)
obtained from James SABOLICK, or 300 Coon Run Road,)
Lower Salem, OH, his vehicle, or the residence of SABOLICK)
located at 7415 Germantown Road, Lower Salem, OH,)
and are currently held at the Washington County Sheriff's)
Office located at 309 Fourth Street in Marietta, Ohio.) Magistrate Judge:

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Kyle Galbreath, a Special Agent with Homeland Security Investigations, being duly sworn, hereby depose and state:

I. EDUCATION, TRAINING AND EXPERIENCE

1. I have been employed as a Special Agent (SA) with the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) since February 2019, and am currently assigned to the Assistant Special Agent in Charge (ASAC) Columbus, Ohio office. I have successfully completed the Criminal Investigator Training program and the HSI Special Agent Training program at the Federal Law Enforcement Training Center in Glynn County, Georgia. Prior to my employment with HSI, I had been employed with the DHS, Customs and Border Protection (CBP), Office of Border Patrol (USBP) from November 2009 to February 2019. In addition, I have received a bachelor's degree in Criminal Justice from Grand Valley State University in Allendale, Michigan.
2. As part of my duties as a Special Agent, I investigate criminal violations relating to human trafficking. Also, I am authorized to investigate criminal violations relating to child exploitation and child pornography violations, including the illegal production, distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A.

II. PURPOSE OF THE AFFIDAVIT

3. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have not withheld any evidence or information which would negate probable cause. I have set forth only the facts necessary to establish probable cause for a search warrant for the content of numerous digital devices that were seized from the person of James **SABOLICK**, the location of 300 Coon Run Road in Lower Salem, Ohio and the residence of **SABOLICK** located at 7415 Germantown Road in Lower Salem, Ohio all of which are currently held in the custody of the Washington County Sheriff's Office located at 309 Fourth Street in Marietta, Ohio (hereinafter referred to collectively as the **SUBJECT DEVICES**).
4. The **SUBJECT DEVICES** to be searched are more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2423 – the production, distribution, transmission, receipt, and/or possession of child pornography, and the transportation of a minor individual for illicit sexual conduct. I am requesting authority to search the entirety of the **SUBJECT DEVICES**, wherein the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

III. APPLICABLE STATUTES AND DEFINITIONS

5. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of

interstate or foreign commerce or in or affecting interstate or foreign commerce.

Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.

6. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct; if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.
7. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.
8. Title 18 U.S.C. § 2423 makes it a federal crime for any person to travel in interstate commerce with a motivating purpose to engage in illicit sexual conduct with another person, including the production of child pornography.
7. The term "child pornography"¹, as it is used in 18 U.S.C. § 2252A, is defined pursuant to 18 U.S.C. § Section 2256(8) as "any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-

¹ The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually conduct.

8. The term "sexually explicit conduct", as used in 18 U.S.C. §§ 2251 and 2252, is defined pursuant to 18 U.S.C. § 2256(2)(A) as "actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person." Pursuant to 18 U.S.C. § 2256(2)(B), "sexually explicit conduct" when used to define the term child pornography, also means "(i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (ii) graphic or lascivious simulated; (I) bestiality; (II) masturbation; or (III) sadistic or masochistic abuse; or (iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person."
9. The term "minor", as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as "any person under the age of eighteen years."
10. The term "visual depiction," as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image."
11. "Graphic" when used with respect to a depiction of sexually explicit conduct, means that viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted. (18 U.S.C. § 2256(10)).
12. The term "computer"² is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

²The term "computer" is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

13. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as printing or typing) or electrical, electronic or magnetic form (such as any and all digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).
14. "Internet Service Providers" (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
15. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.
16. As it is used throughout this affidavit and all attachments hereto, the term "storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

**IV. BACKGROUND REGARDING COMPUTERS, DIGITAL STORAGE DEVICES,
THE INTERNET**

17. I know from my training, experience, and information provided to me by other law enforcement agents, that computer hardware, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software,

and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.

18. Computers, mobile devices and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.
19. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.
20. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.
21. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 32GB. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 4 Gigabytes to 256

Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 4 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

22. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of

- log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses³ and other information both in computer data format and in written record format.
23. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user's true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.
24. It is often possible to recover digital or electronic files, or remnants of such files, months or even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
25. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of

an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

26. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.
27. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

28. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:
- a) Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This

sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b) Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

29. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU) as well as all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

VI. INVESTIGATION AND PROBABLE CAUSE

30. On July 24, 2021, at approximately 3:12am, the Marietta Police Department (MPD) initiated a traffic stop on I-77 South in Marietta, Ohio on a 2004 Mercury Mountaineer, bearing Ohio registration JFS4611. Despite MPD activating their emergency equipment, the driver of that SUV, now known as James SABOLICK, continued driving away from MPD, crossing over a bridge before ultimately coming to a stop in West Virginia. The bridge SABOLICK crossed runs over the Ohio River and connects the state of Ohio to the state of West Virginia.

31. After stopping SABOLICK's vehicle, MPD approached the SUV and observed an individual attempting to conceal themselves in the backseat. When asked if anyone else was inside the SUV, SABOLICK initially indicated he was alone. He ultimately changed

- his story and then admitted that there was another individual inside the vehicle. MPD identified that individual as a 17-year-old female (hereinafter referred to as Minor Victim).
32. Law enforcement with the Southeastern Ohio Human Trafficking Task Force from the Washington County Sheriff's Office (WCSO) then arrived on scene. An initial interview with Minor Victim was then conducted. In that interview, Minor Victim confirmed that she and SABOLICK had been having sex and indicated that this had occurred five or more times. WCSO learned the Minor Victim had snuck out of her residence in Walker, West Virginia to have sex with SABOLICK. Minor Victim confirmed that SABOLICK picked her up near her residence in West Virginia and then subsequently took her to a cabin located near his residence in Ohio.
33. SABOLICK was then placed under arrest for Obstructing Official Business and Failure to Signal. Recovered on his person was a Samsung cellphone in a blue case, an Apple iPhone in a black case, and a USB flash drive, all of which are included in the list of SUBJECT DEVICES in Attachment A.
34. Upon his arrest, SABOLICK was interviewed by WCSO. After being read his Miranda rights, SABOLICK told law enforcement that the Minor Victim was 17 years old. He admitted he "went down [to West Virginia] and got her" and stated that he then took Minor Victim to a hunting cabin near his residence. He also admitted to receiving nude pictures of the Minor Victim in the past as well as possessing nude pictures of the Minor Victim on his cellphone. In addition, SABOLICK also admitted to communicating with Minor Victim on the phone.
35. During the course of the conversation with WCSO, SABOLICK consented to his Samsung cellphone being searched. During a cursory review by WCSO, several photographs depicting Minor Victim nude were observed on his Samsung cellphone. In one of the photographs, Minor Victim is observed with a large serving spoon inserted into her anus. The investigation revealed that the photographs of Minor Victim that were observed were taken at the hunting cabin SABOLICK had referenced, located at 300 Coon Run Road in Lower Salem, Ohio.
36. On July 24, 2021, a forensic interview of Minor Victim was completed. During that interview, Minor Victim stated around midnight [July 24, 2021], SABOLICK picked her up from her residence in Walker, West Virginia and took her to a cabin in Ohio (later

identified as 300 Coon Run Rd. Lower Salem, Ohio). While at the cabin on Coon Run Road, Minor Victim stated that she and SABOLICK engaged in oral, vaginal, and anal sex. Minor Victim also revealed SABOLICK poked her nipples with a sewing needle, used a lighter to burn her nipples, pulled her hair, used panty hose to tie her up and strangle her, inserted an object in her anus, had the Minor Victim drink his urine, and then urinated in Minor Victim's mouth and on her body. Minor Victim also confirmed that SABOLICK photographed her nude body and genitalia during this encounter using his phone. Minor Victim also confirmed that she and SABOLICK had engaged in sex acts in both the state of West Virginia and the state of Ohio.

37. In the interview, Minor Victim further revealed that the previous year, she and SABOLICK had sex on a vehicle while it was parked in West Virginia and that while they had sex, Minor Victim's 10-year-old sister watched. Minor Victim stated that SABOLICK told her that her sister was "kinky." Minor Victim also stated that SABOLICK then told her younger sister "I might do this to you one day."
38. When asked how Minor Victim and SABOLICK communicated, Minor Victim stated that she both called and texted with SABOLICK using her cellphone. In addition, Minor Victim indicated that she also communicated with SABOLICK on the social media applications Instagram and Facebook.
39. WCSO then added the charges of Pandering Sexually Oriented Material Involving a Minor, Possession of Criminal Tools, Interference with Custody/Taking a Child Across State Lines to SABOLICK's arrest.
40. On July 24, 2021, a search warrant was executed at 300 Coon Run Road in Lower Salem, Ohio. Law enforcement observed the structure to be the hunting cabin where SABOLICK took Minor Victim to engage in sexual intercourse. The investigation also revealed that the interior of the cabin matched the background of the sexually explicit photographs taken of Minor Victim that were recovered on SABOLICK's Samsung cellphone. WCSO seized numerous items from the hunting cabin, including a black plastic spoon which appeared to be the same spoon that had been inserted into the anus of the Minor Victim which was depicted in a photograph that had been reviewed by law enforcement. Also seized were soiled paper towels/napkins, a black and gray spatula, a deer blanket, and a white pill

capsule. In addition to the items seized, photographs were taken of the interior of the hunting cabin.

41. During the course of the investigation, law enforcement learned that SABOLICK resided at 7415 Germantown Road in Lower Salem, Ohio. Specifically, a record check through the Ohio Bureau of Motor Vehicles (BMV) revealed that SABOLICK had registered the 7415 Germantown Road address on his driver's license and, in addition, registered a 2004 Mercury Mountaineer with Ohio license plate JFS4611 with that same address. The 2004 Mercury Mountaineer registered to SABOLICK was the same vehicle he was driving when he was arrested. Furthermore, a state of Ohio certificate of title was found during a search of SABOLICK's vehicle. The certificate of title listed SABOLICK with address 7415 Germantown Road Lower Salem, Ohio as the owner of the 2004 Mercury Mountaineer.
42. On July 24, 2021, an additional search warrant was executed at the 7415 Germantown Road residence belonging to SABOLICK. Pursuant to that search warrant, numerous items were seized including panty hose, a blue 160 GB external hard drive, a USB and flash drive, an Xbox 360, a mobile phone, a Dell laptop, a Dell laptop with external hard drive, address books, and an ASUS tablet. All of the digital media devices seized from SABOLICK's residence are included in list of **SUBJECT DEVICES** in Attachment A.
43. On July 27, 2021, a search warrant was also obtained for the three digital media devices recovered from SABOLICK's person the night of his arrest. More specifically, the search warrant related to the Samsung cellphone in a blue case, an Apple iPhone in a black case, and a USB flash drive all of which are again included in the list of **SUBJECT DEVICES** listed in Attachment A.
44. Finally, on July 28, 2021, WCSO executed a search warrant on the 2004 Mercury Mountaineer, bearing Ohio registration JFS4611, which is the vehicle SABOLICK was driving the Minor Victim in the night of his arrest. Recovered from that Mercury Mountaineer were numerous items, including panty hose, lubricant, white towels, a twisted tea can, and a box of t-pins.
45. On July 29, 2021, your affiant met with WCSO and the Southeastern Human Trafficking Task Force and was briefed on their investigation. Your affiant viewed several images that depicted Minor Victim in a state of nudity that appeared to be taken at the cabin located at 300 Coon Run Road in Lower Salem, Ohio. During the communications with WCSO and

the Southeastern Human Trafficking Task Force, a request for assistance was made in the ongoing investigation of SABOLICK, including conducting further examinations and continuing forensic analysis of the SUBJECT DEVICES.

46. All of the SUBJECT DEVICES listed in Attachment A were seized from the person of SABOLICK; or the hunting cabin visited by SABOLICK or the residence of SABOLICK during the execution of the search warrants by WCSO described above. All of those devices were subsequently transported to the Washington County Sheriff's Office in Marietta, Ohio, and have remained in law enforcement custody since the time they were seized. Your affiant knows that any forensic examinations that may have been conducted of some of the SUBJECT DEVICES have not altered the data contained in the SUBJECT DEVICES at the time they were seized, and that the SUBJECT DEVICES remain in the same state, for purposes of this investigation, as they were at the time they were seized.
47. Based on the information that had been gathered to date by WCSO, combined with your affiant's belief that SABOLICK likely possesses the characteristics common to individuals with a sexual interest in minors, as described below, your affiant believes that there is probable cause that the SUBJECT DEVICES contain evidence of SABOLICK's child pornography and child exploitation activities.

VII. SEARCH METHODOLOGY TO BE EMPLOYED

48. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans, downloading or copying of the entire device, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. Specifically, such techniques may include, but are not limited to:
 1. Examination of all of the data contained in any computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items listed in Attachment B;
 2. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items in Attachment B;

3. Surveying various files, directories and the individual files they contain;
4. Opening files in order to determine their contents;
5. Scanning storage areas;
6. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
7. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

49. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

VIII. COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

50. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who have a sexual interest in children and who produce, distribute, and receive child pornography:

- a) Those who have a sexual interest in children and who produce, distribute, and receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b) Those who have a sexual interest in children and who produce, distribute, and receive child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

- c) Those who have a sexual interest in children and who produce, distribute, and receive child pornography often times possess and maintain any "hard copies" of child pornographic material that may exist, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years. More recently, however, it has become more common for people who have a sexual interest in children to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.
- d) Likewise, those who have a sexual interest in children and who produce, distribute, and receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.
- e) Those who have a sexual interest in children and who produce, distribute, and receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and sometimes maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- f) Those who have a sexual interest in children and who produce, distribute, and receive child pornography rarely are able to abstain from engaging in sexual exploitation of children or child pornography activities for any prolonged time period. This behavior

has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.

51. When images and videos of child pornography are produced and stored on computers and related digital media, forensic evidence of the production, distribution, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.
52. Based upon the conduct of individuals who have a sexual interest in children and who produce, distribute, and receive child pornography set forth in the above paragraphs, namely, that they tend to maintain their collections at a secure, private location for long periods of time, that they rarely are able to abstain from child pornography activities for a prolonged period of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2423 – the production, distribution, transmission, receipt, and/or possession of child pornography, and the transportation of a minor individual for illicit sexual conduct, is currently located on the **SUBJECT DEVICES**.

IX. CONCLUSION

53. Based on all the forgoing factual information, there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252, and 2423 – the production, distribution, transmission, receipt, and/or possession of child pornography, and the transportation of a minor individual for illicit sexual conduct, have been committed and that evidence, fruits and instrumentalities of these offenses will be found within the **SUBJECT DEVICES** listed in Attachment A, which is incorporated herein by reference. Your affiant therefore respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT DEVICES** described in Attachment A, and the seizure of the items described in Attachment B.



Kyle Galbreath
Special Agent
Homeland Security Investigations

Sworn to and subscribed before me this 2nd day of September, 2021.



Kimberly A. Johnson

United States Magistrate Judge



ATTACHMENT A
PROPERTY TO BE TO BE SEARCHED

The devices to be searched are the following:

1. One Samsung cellphone in blue case (WCSO tracking # 32477).
2. One Apple iPhone in black case (WCSO tracking # 32478).
3. One USB Device (WCSO tracking # 32479).
4. One external hard drive (WCSO tracking # 32486).
5. One USB and flash drive (WCSO tracking # 32487).
6. One Xbox360 (WCSO tracking # 32488); .
7. One BS mobile cellphone (WCSO tracking # 32489).
8. One Dell laptop computer (WCSO tracking # 32490).
9. One Dell laptop computer with external hard drive (WCSO tracking # 32491).
10. One ASUS Verizon Tablet (WCSO tracking # 32493).

The items described above were seized from the person of **SABOLICK**; or the hunting cabin visited by **SABOLICK** located at 300 Coon Run Road in Lower Salem, Ohio or the residence of **SABOLICK** located at 7415 Germantown Road, Lower Salem, Ohio, pursuant to multiple search warrants and are currently being held at the Washington County Sheriff's Office secure evidence storage location at 309 Fourth St. Marietta, OH.

This warrant authorizes the forensic examination of the **SUBJECT DEVICES** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2251, 2252, and 2423 – the production, distribution, transmission, receipt, and/or possession of child pornography, and the transportation of a minor individual for illicit sexual conduct, those violations involving James SABOLICK, including:

1. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or online storage or chat programs), utilities, compilers, interpreters, and communications programs.
2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs, and electronic messages,) pertaining to the production, possession, receipt, or distribution of child pornography.
3. In any format and medium, all originals, computer files, copies, and negatives of child pornography and child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to digital files, e-mail messages, chat logs and electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by cellular phone or computer, any child pornography.
5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications related to the sexual abuse or exploitation of minors.

6. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider or Electronic Communications Service.
7. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
8. Any and all visual depictions of minors, whether clothed or not, for comparison to any child pornography or child erotica found during the execution of this search warrant or obtained during the course of this investigation.
9. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.
10. Any Internet or cellular telephone communications (including email, social media, online chat programs, etc.) with others in which child exploitation materials and offenses are discussed, posted, and/or traded;
11. Any Internet or cellular telephone communications (including email, social media, etc.) with minors;
12. Evidence of the utilization of peer-to-peer file sharing programs;
13. Evidence of utilization of user names or aliases, email accounts, social media accounts, and online chat programs, and usernames, passwords, and records related to such accounts;
14. Evidence of software that would allow others to control the SUBJECT DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the

- presence or absence of security software designed to detect malicious software and evidence of the lack of such malicious software;
15. Evidence indicating the computer user's state of mind as it relates to the crimes under investigation;
 16. Evidence that any of the **SUBJECT DEVICES** were attached to any other digital device or digital storage medium;
 17. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the **SUBJECT DEVICES**;
 18. Passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT DEVICES**;
 19. Records of or information about Internet Protocol addresses used by the **SUBJECT DEVICES**;
 20. Records of or information about any Internet activity occurring on the **SUBJECT DEVICES**, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.